

Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) Standards Review

CSWG Standards Review Report on

*Security Assessment of SAE J2836-1: Use Cases for
Communication Between Plug-in Vehicles and the Utility Grid*

November 12, 2010

Security Assessment of SAE J2836-1: Use Cases for Communication Between Plug-in Vehicles and the Utility Grid

1. Introduction

1.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different “layers” in the communications “stack” or “profile,” one example of such a profile is the Grid Wide Architecture Council (GWAC)¹ Stack. Some standards address the lower layers of the communications stack, such as wireless media, fiber optic cables, and power line carrier. Others address the “transport” layers for getting messages from one location to another. Still others cover the “application” layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Since they are abstract, cybersecurity technologies cannot be linked to them until they are translated into “bits and bytes” by mapping them to one of the semantic structures. Above the communications standards are other security standards that address business processes and the policies of the organization and regulatory authorities.

Secondly, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. In addition, cybersecurity must address those aspects outside of the communications system in the upper GWAC Stack layers that may just be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to: cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Thirdly, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself: how and where a standard is used must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC Stack may address issues of data importance.

Fourthly, some standards do not mandate their provisions using “shall” statements, but rather use statements such as “should,” “may,” or “could.” Some standards also define their provisions as being “normative” or “informative.” Normative provisions often are expressed with “shall” statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the “shall,” “should,” “may,” and/or “could” statements, “normative,” or “informative” language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or “profile” of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of a stack of

¹GridWide Architecture Council, http://www.gridwiseac.org/pdfs/interopframework_v1.pdf

policy, procedural, and communication standards designed to provide specific services. Ultimately, cybersecurity as applied to the information exchange standards should be described as profiles of technologies and procedures which can include both “power system” methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if TCP/IP is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then TLS (transport layer security) should most likely (but not absolutely) be used. For some specific Smart Grid communication standards, such as International Electrotechnical Commission (IEC) 61850 and IEC 60870-6, specific cybersecurity standards (IEC 62351 series) were developed to meet typical implementations of these standards.

In the following discussions of information exchange standard(s) being reviewed, these caveats should be taken into account.

1.2 Standardization Cycles of Information Exchange Standards

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as “appropriate security technologies and procedures should be implemented.”

With the advent of the Smart Grid, cybersecurity has become increasingly important within the utility sector. However, since the development cycles of communication standards and cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

1.3 References and Terminology

References to the National Institute of Standards and Technology (NIST) security requirements refer to the NIST Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, Chapter 3, High-Level Security Requirements.

References to “government-approved cryptography” refer to the list of approved cryptography suites identified in Chapter 4, Cryptography and Key Management, of NISTIR 7628. Summary tables of the approved cryptography suites are provided in Chapter 4.3.2.1.

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees²:

¹ Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after “which”) comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

Requirements are expressed by “...shall...,” which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall equals is required to*).

Recommendations are expressed by “...should...,” which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should equals is recommended that*).

Permitted or allowed items are expressed by “...may...,” which is used to indicate a course of action permissible within the limits of the standard (*may equals is permitted to*).

Ability to carry out an action is expressed by “...can ...,” which is used for statements of possibility and capability, whether material, physical, or causal (*can equals is able to*).

The use of the word *must* is deprecated, and should not be used in these standards to define mandatory requirements. The word *must* is only used to describe unavoidable situations (e.g. “All traffic in this lane must turn right at the next intersection.”)

2. SAE J2836-1: Use Cases for Communication Between Plug-in Vehicles and the Utility Grid

2.1 Description of the Document

The use cases described in this document identify the equipment (system elements) and interactions to support grid-optimized AC or DC energy transfer for plug-in vehicles.

Use cases are technology-neutral, leaving implementers free to choose technological solutions appropriate to specific scenarios. For example, depending upon the situation, communication may occur via local wireless (ZigBee, Wi-Fi, etc.), power-line carrier (e.g., HomePlug PLC), vehicle telematics, long-range wireless (GSM, CDMA, WiMax, etc.), Internet protocols, or a combination of these methods.

2.2 Assumptions and Issues

This document provides Use Cases, essentially at the Business Procedures and Business Context layers of the GWAC stack. These Use Cases are technology-neutral, so no specific security technologies are addressed. However, these Use Cases also do not address the security requirements from a business perspective.

2.3 Summary of Cybersecurity Content

2.3.1 Does the standard address cybersecurity? If not, should it?

The document mentions cybersecurity in some places.

In the definitions of the Actors, some in Section 2.1 and others in many of the Use Cases described in Appendices A & B, the following references to security are made:

- The Energy Services Communication Interface (ESCI) definition makes a “shall” statement on security: “*ESCI shall employ appropriate security policies when communicating demand side management program-related messages.*” This is stated again in slightly different words in Appendices A and B in various Use Case steps.

- The ESI definition states, “*Energy Services Interface – Provides security and, often, coordination functions that enable secure interactions between relevant HAN Devices and the Utility.*” This statement is reiterated with slightly different words in Section 3.2.1.
- The End Use Measurement Device (EUMD) definition states, “*End Use Measurement Device shall employ appropriate security policies when communicating demand side management program-related messages.*”

Although it is valid for Use Case documents not to discuss security technologies, it is important for some Use Cases to directly address the security requirements at a “business” or functional level – identifying what types of information should be confidential, what data integrity issues need to be addressed, what availability and performance requirements must drive configurations, and what potential privacy issues must be understood. These types of security Use Cases have not been included in this document.

2.3.2 What aspects of cybersecurity does the standard address and how well (correctly) does it do so?

The correlations between this document and the security requirements described in NISTIR 7628, *Guidelines to Smart Grid Cybersecurity*, Chapter 3, families and requirements, are shown in Table 1:

Table 1: Correlations between Standard being Assessed and the NISTIR Security Requirements

Reference in Standard ³	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
Definitions of Actors: ESCI, ESI, and EMUD	References to Security Policies, without identifying which ones	These references are too vague to be useful from a security perspective

2.3.3 What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?

The following aspects of security are not covered within the use cases:

- The use cases do not cover any cybersecurity related use cases, such as key management, secure upgrade of the software, and validation of the authenticity of the system and its components.
- The use cases do not discuss cybersecurity services or requirements.
- The use cases do not discuss the privacy of customer information during the business process.

It is recommended that this document be accepted as is, but that corresponding documents be developed in future efforts (in a DEWG or PAP) that:

- Develop additional cybersecurity Use Cases during the next V2G PAP and/or DEWG efforts.
- Review the normative and informative reference document list within SAE J2836/1 to determine if any cyber security requirements in those documents need to be updated or enhanced.

³ The references may be just the section numbers or could include the title of the section

2.3.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

No known activity at this time, although it is expected that either a new PAP or DEWG will be formed.

2.3.5 List any references to other standards and whether they are normative or informative.

2.3.5.1 Normative References

- SAE J1772™ SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler

2.3.5.2 Informative References

- SAE J2293/1 Energy Transfer System for Electric Vehicles - Part 1: Functional Requirements and System Architectures
- SAE J2293/2 Energy Transfer System for Electric Vehicles - Part 2: Communication Requirements and Network Architecture
- <http://www.utilityami.org/docs/UtilityAMI%20HAN%20SRS%20-%20v1.04%20-%20080819-1.pdf>
- <http://zigbee.org/Markets/ZigBeeSmartEnergy/ZigBeeSmartEnergyOverview/tabid/431/Default.aspx>